Trojanisches Pferd

Als Trojanisches Pferd (kurz „Trojaner“) bezeichnet man ein Computerschadprogramm, das sich als nützliche Anwendung tarnt. Es wird gezielt eingeschleust, kann aber auch zufällig auf einem Computer landen. Sie sind oft in Mailanhängen versteckt.

Funktionsweise

Ein Trojanisches Pferd zählt zur so genannten Malware, also unerwünschten Programmen. Der Name ist aus der griechischen Mythologie abgeleitet, in der das hölzerne „Trojanische Pferd“ von den Griechen dazu genutzt wurde, getarnt in einen geschützten Bereich, die Festung von Troja, vorzudringen und den Krieg so zu gewinnen.
Als Schadprogramme auf den PC gelangen Trojaner über Anhänge von E-Mails oder über Tauschbörsen. Ein Trojanisches Pferd richtet Schaden von innen an, indem es auf dem Computer heimlich weitere Programme installiert. Beispiele sind „Sniffer“ oder „Keylogger“, Spionageprogramme, die Tastatureingaben aufzeichnen. Aber auch sogenannte Backdoorprogramme werden eingeschleust. Mit denen kann ein Computer unbemerkt über das Internet ferngesteuert werden. Mit Hilfe von Trojanern werden Daten und Passwörter ausspioniert und online versendet, ebenso wie Spam-Mails. Es können auch Systemkonfigurationen verändert oder gelöscht werden. Trojaner müssen nicht zwangsläufig ein Schadprogramm installieren. Allerdings sind es immer Programme, denen eine versteckte Funktion hinzugefügt wurde.

Tückischer „Polizei“-Trojaner

Im Sommer 2012 kursierte eine neue Variante einer Schadsoftware mit den Logos des Bundesamtes für Sicherheit in der Informationstechnik, der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen und der Bundespolizei. Darin gaben Kriminelle vor, die genannten Stellen hätten den Computer aus Sicherheitsgründen gesperrt. Zum Beispiel, weil vermeintlich Raubkopien oder Kinderpornographie gefunden worden seien. Der PC-Bildschirm wurde gesperrt und der Benutzer aufgefordert, ein Bußgeld von 100 Euro zu überweisen. Das landete dann auf dem Konto der Betrüger. Zum Entfernen des Trojanischen Pferdes empfiehlt das BSI das DE-Cleaner-Rettungssystem und die Kaspersky Rescue Disk.
Weitere Tipps liefert das Anti-Bot-Beratungszentrum vom Verband der deutschen Internetwirtschaft e.V. mit Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik.

Schutz vor Trojanischen Pferden:

- keine Mail-Anhänge von unbekannten Absendern öffnen
- keine Software aus unbekannten Quellen auf den Computer laden
- einen Virenscanner verwenden
- Sicherheitseinstellungen des Internet Explorer kontrollieren

Zurück